

UNITED STATES DISTRICT COURT

for the
Western District of Washington

| | |
|---|--------|
| FILED | LODGED |
| RECEIVED | |
| Mar 17, 2023 | |
| CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA | |
| BY | DEPUTY |

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
Information Associated with Certain Cellular Towers

Case No. MJ23-5083

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is incorporated herein by reference
located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

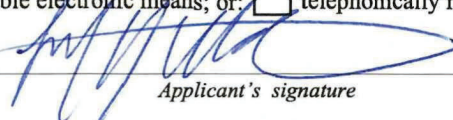
| Code Section | Offense Description |
|----------------|---------------------------|
| 18 U.S.C. 1366 | Damage to Energy Facility |
| 18 USC 371 | Conspiracy |

The application is based on these facts:

- ☒ See Affidavit of Special Agent Samuel Wharton continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Samuel Wharton, Special Agent, FBI
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/17/2023


Judge's signature

City and state: Seattle, Washington

Theresa L. Fricke, United States Magistrate Judge
Printed name and title

ATTACHMENT A**Property to Be Searched**

This Order applies to certain records (Voice, SMS and DATA connections) and information in the possession of T-Mobile, a cellular service provider headquartered in Bellevue, Washington, related to the following addresses of interest and those cellular telephone towers providing service to the below addresses during the listed dates and times. Please provide all the cellular telephone numbers whose timing advance data places them within a one-half mile radius from the below locations.

| <u>Cell Towers</u> | <u>Dates</u> | <u>Times (PDT)</u> |
|---|--|---|
| The cell towers that provided cellular service to 2210 Robinson Road, Woodland, WA 98674 | November 17, 2022 | 3:30 a.m. – 3:45 a.m. (PST) 5:00 a.m. – 6:00 a.m. (PST) |
| The cell towers that provided cellular service to 220 North Pekin Road, Woodland, WA 98674 | November 18, 2022 | 4:00 a.m. – 5:00 a.m. (PST) |
| The cell towers that provided cellular service to 1007 39 th Ave SE, Puyallup WA 98374 | November 19, 2022 to November 20, 2022 | 11:00 p.m. (11/19/22) through 5:00 a.m. (11/20/22) (PST) |
| The cell towers that provided cellular service to 1669 2 nd Avenue SW, Tumwater WA 98512 | November 22, 2022 | 3:45 a.m. – 5:00 a.m. (PST) |
| The cell towers that provided cellular service to 16885 South Eaden Road, Oregon City, OR 97045 | November 24, 2022 | 12:50 a.m. to 1:50 a.m. (PST) |
| The cell towers that provided cellular service to 8396 SE Sunnyside Road Clackamas, OR 97015 | November 28, 2022 | 12:30 a.m. to 1:10 a.m. (PST) |

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

For each cell tower described in Attachment A, T-Mobile is required to disclose to the United States records and other information (not including the contents of communications) about all communications made using the cellular towers identified in Attachment A during the corresponding timeframes listed in Attachment A, including records that identify:

- a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower (“the locally served wireless device”) that registered with the cell tower, including Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), and International Mobile Equipment Identities (“IMEI”);
- b. the source and destination telephone numbers associated with each communication (including the number of the locally served wireless device and the number of the telephone that called, or was called by, the locally served wireless device);
- c. The date, time, and duration of each communication;
- d. for each communication, the “sectors” (i.e. the faces of the towers) that received a radio signal from the locally served wireless device;
- e. the date, time, and duration of each communication;
- f. the type of communication transmitted through the tower (such as voice, sms and data);
- g. the approximate range of the target handsets from the cell tower (commonly referred to as range to tower, Real Time Tool (RTT), or per-call data measurement data, timing advance, True Call or NELOS); and

1 h. the requested order should include all technologies (I.E.2G, 3G, 4G, and LTE).

2 These records should include records about communications that were initiated before
3 or terminated after the timeframe(s) identified in Attachment A if some part of the
4 communication occurred during the relevant timeframe(s) listed in Attachment A.

5 **II. Information to be Seized by the Government**

6 All information described above in Section I that constitutes evidence of violations of
7 Title 18, United States Code, Section 1366 (Destruction of an Energy Facility) and Title 18,
8 United States Code, Section 371 (Conspiracy) during the period of November 17-28, 2022.

9
10 Law enforcement personnel (who may include, in addition to law enforcement
11 officers and agents, attorneys for the government, attorney support staff, agency personnel
12 assisting the government in this investigation, and outside technical experts under
13 government control) are authorized to review the records produced by the Provider in order
14 to locate the things particularly described in this Warrant.

AFFIDAVIT OF SAMUEL WHARTON

STATE OF WASHINGTON)
) ss.
 COUNTY OF THURSTON)

I, Samuel Wharton, a Special Agent with the Federal Bureau of Investigation, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 2017. My current assignment is with the FBI Seattle Field Office, South Sound Joint Terrorism Task Force, investigating a variety of criminal and national security matters, including violent crimes and major offenses such as threats to human life, threats to damage property, actual and attempted bombings, and efforts to use violence in support of, or to counter, a particular ideology. My training and experience include a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable cause. As an FBI agent, I have investigated several criminal violations, including narcotics trafficking, homicide, and international and domestic terrorism. I have also served as the affiant for search warrants, including search warrants for electronic evidence.

The facts set forth in this Affidavit are based on my personal knowledge; knowledge obtained from other individuals during this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for search warrants, it does not set forth every fact that I, or others, have learned during this investigation.

//

//

PURPOSE OF AFFIDAVIT

I make this affidavit in support of an application for warrants for records and information associated with certain cellular towers (“cell towers”). The purpose of the warrants is to identify suspects who engaged in violations of Title 18, United States Code, Sections 1366 and 371 (Conspiracy to Damage Energy Facilities). The cell tower data is expected to allow investigators to identify the phones used by the subjects at the time of the offenses, which may allow investigators to identify the subjects themselves. The information requested is in the possession, custody, and/or control of T-Mobile, a cellular service provider headquartered in Bellevue, Washington.

This warrant request is a follow-up to a prior cell tower warrant issued by this Court. On December 16, 2022, Magistrate Judge J. Richard Creatura issued a cell tower warrant in case MJ22-5295. On January 30th, 2022, the FBI received the returns from T-Mobile, in case reference number 4163401. In the original warrant, we failed to request for T-Mobile to provide what is known as “timing advance measurement data.” This data, as explained below, is more comprehensive than the other types of cell tower data that was requested in our original warrant. The purpose of this follow-up warrant is to add the request for timing advance measurement data in order to further investigate the identities of the potential perpetrators of the offenses under investigation.

JURISDICTION

This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTE

Title 18, United States Code, Section 1366 defines offenses for causing destruction to an “energy facility.” Section (a) of the statute makes it a felony offense where one “knowingly and willfully damages or attempts or conspires to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been

completed, or if the object of the conspiracy had been achieved, have exceeded \$100,000, or damages or attempts or conspires to damage the property of an energy facility in any amount and causes or attempts or conspires to cause a significant interruption or impairment of a function of an energy facility.” Section (b) defines a lesser-included felony offense where one “knowingly and willfully damages or attempts to damage the property of an energy facility in an amount that in fact exceeds or would if the attempted offense had been completed have exceeded \$5,000.” The term “energy facility” is defined as “a facility that is involved in the production, storage, transmission, or distribution of electricity, fuel, or another form or source of energy, or research, development, or demonstration facilities relating thereto . . .” 18 U.S.C. § 1366(c).

BACKGROUND RELATING TO CELL TOWERS

In my training and experience, I have learned that T-Mobile is a company that provides cellular communications service to the public. To provide this service, many cellular service providers maintain antenna towers (“cell towers”) that serve and provide cellular service to devices that are within range of the tower’s signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data. When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it.

Based on my training and experience, I also know that each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment

1 Identity (“IMEI”). The types of identifiers assigned to a given cellular device are dependent
2 on the device and the cellular network on which it operates.

3 Based on my training and experience, I know that cellular providers such as T-Mobile
4 routinely and in their regular course of business maintain historical records that allow them
5 to determine which wireless devices used cellular towers on the cellular provider’s network
6 to send or receive communications. For each communication sent or received via the
7 wireless provider’s network, these records may include: (1) the telephone call number and
8 unique identifiers of the wireless device that connected to the provider’s cellular tower and
9 sent or received the communication (“the locally served wireless device”); (2) the cellular
10 tower(s) on the provider’s network, as well as the “sector” (*i.e.*, face of the tower) to which
11 the locally served wireless device connected when sending or receiving the communication;
12 and (3) the date, time, and duration of the communication.

13 Based on my training and experience, I know that cellular providers such as T-Mobile
14 can query their historical records to determine which cellular device(s) connected to a
15 particular cellular tower during a given period of time and to produce the information
16 described above. I also know that cellular providers can determine which cellular tower(s)
17 provided coverage to a given location at a particular time.

18 Based on my training and experience and the above facts, information obtained from
19 cellular service providers such as T-Mobile that reveals which devices used a particular cell
20 tower (and, where applicable, sector) to engage communications can be used to show that
21 such devices were in the general vicinity of the cell tower at the time the communication
22 occurred. Thus, the records requested in this case may identify the cellular devices that were
23 in the vicinity of the victim energy facilities at the time of the offenses. This information, in
24 turn, will assist law enforcement in determining which persons were present for those
25 offenses.

26 Based on my training and experience, I also know that T-Mobile collects timing
27 advance measurement data in the normal course of business. Timing advance data estimates
28 the approximate distance of the cellular device from a cellular tower based upon the speed

1 and time that it takes the cellular signals to travel from the cell tower to the device and back
2 to the tower. This information can be used to estimate the approximate location range. These
3 measurements are more precise than typical cell site records contained in call detail records.
4 This data helps identified the devices that are located very close to the cell tower and those
5 located at a greater distance.

6 T-Mobile can provide timing advance data for all the devices connected to a cell
7 tower for a specific time frame. A traditional tower dump includes only the cell tower and
8 sector (no distances) data and only covers voice and SMS connections. Timing advance data
9 often includes voice, SMS, and data activity. Users of cell phones are more actively engaged
10 in data connections than voice and SMS activity.

11 Based on my training and experience, I know that a large percentage of people whose
12 cellular devices connect to a cell tower as they pass within range may not be actively using
13 their devices to make calls or send text messages, but their devices will still connect to the
14 tower and utilize it for passive data connections. These devices would be identified through
15 timing advance data, but not through the previous cell tower data we requested, which would
16 only capture more active utilization of the tower through SMS or phone calls.

17 Based on my training and experience, I know that individuals engaged in criminal
18 activity do not typically pause or stop during that activity to make phone calls or send text
19 messages. However, in the process of carrying out criminal acts, their cellular devices still
20 connect to the cell towers that serve the area they are in, and through data connections, are
21 still captured in timing advance data.

22 **SUMMARY OF PROBABLE CAUSE**

23 **Extremist Propaganda Calling for Attacks on Energy Facilities**

24 In July 2022, a publication was released online entitled “The Hard Reset.” This
25 publication was distributed by groups and individuals that espouse a Racially or Ethnically
26 Motivated Violent Extremist (RMVE) ideology. The publication promotes an ideology
27 known as “accelerationism,” which is the idea that society and/or nation states are headed for
28 an inevitable collapse and accelerationists should not wait for the collapse but should take

1 actions to accelerate the collapse. Once this collapse occurs, RMVE groups could then start a
2 race war and establish a white ethnostate.

3 The “Hard Reset” publication includes detailed technological specifications
4 regarding different types of critical infrastructure, including water treatment plants, bridges,
5 railways, and energy facilities (such as electric substations), and their vulnerabilities. The
6 publication also provides detailed instructions on how “saboteurs” could best exploit these
7 vulnerabilities to damage or destroy these facilities. The publication advocates for saboteurs
8 to take steps to locate these facilities of critical infrastructure, identify their weak points, and
9 attack them to inflict substantial damage using firearms, arson, and other means.

10 Relevant to this investigation, the “Hard Reset” publication encourages followers to
11 attack energy facilities and, specifically, electrical substations, stating: “Electricity is the
12 main satiating tool the system uses to keep the masses from rioting. ... Without power other
13 types of sabotage become very powerful and harder to repair, as such the impact of a
14 directed outage could exponentially increase the results of a saboteur’s efforts.” Regarding
15 electrical substations, the publication states:

16 Substations are a pillar of the electrical grid, responsible for the distribution,
17 transmission, collection, switching, and conversion depending on the type.
18 Substations are publicly indexed and generally easy to find with any map
19 service. Some services will even provide additional information about a
20 substation. Google street view should be utilized. A saboteur should aim for
21 specific targets while shooting at substations. The breaker is one such target,
22 itself being a giant sophisticated fuse for dealing with large amounts of voltage
23 when things go wrong elsewhere in the power grid. They result on filling a
24 chamber with a non-conductive oil or gas in order to cut current off. They
25 won’t be able to function without their oil. And can catch fire...aim for
26 damage to result not from electrical fires or faulting, but from overheating and
27 oil fires. Radiators and cooling fans, pictured below, should also be targeted.
28 Other targets include oil pumps, oil conservator tank, and electronic controls.

25 The publication includes detailed photographs of transformers and other electrical
26 equipment, with their component parts labeled.

1 In recent months, there have been multiple incidents during which energy facilities in
2 Southwest Washington and Northwest Oregon have been damaged using firearm, blunt
3 objects, and/or arson. These incidents are described below.

4 **Location 1: 2210 Robinson Road Woodland, Washington**

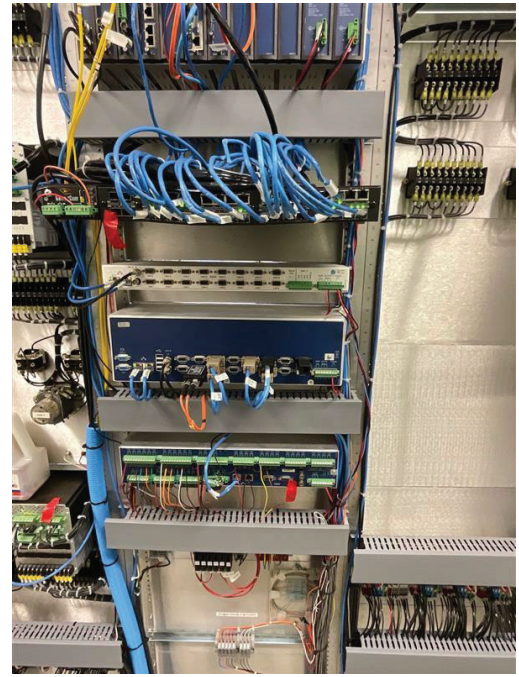
5 On November 17, 2022, unknown subjects caused damage to the electric substation
6 located at 2210 Robinson Road, Woodland, Washington 98674. This substation is owned
7 and managed by the Cowlitz Public Utility District and receives its electricity from the U.S.
8 Department of Energy, Bonneville Power Administration. The substation is responsible for
9 distributing electricity to the town of Woodland and the surrounding areas.

10 On November 17, 2022, the unknown suspects cut their way through a barbed wire
11 perimeter fence surrounding the substation. Once inside the yard, these individuals broke a
12 window to gain access to the yard's control house.



23 Inside the control house, they manually manipulated the breakers that control the
24 flow of electricity. Using a blunt object, the suspects also smashed the exposed, inner
25 workings of the breaker towers, rendering multiple components inoperative and in need of
26 either repair or replacement. This offense caused the interruption of electrical service for
27 approximately 1,900 customers and set-off alarms at the Cowlitz Public Utility District
28

1 Headquarters. The Cowlitz Public Utility District estimates that the damage caused by this
2 incident was between \$50,000 and \$60,000.



3
4
5
6
7
8
9
10
11
12
13
14
15 I have reviewed security footage from Woodland High School, which is located near
16 the substation. Based on my review of security footage, at around 3:37 a.m. on November
17 17, 2022, a dark colored sedan drives slowly in and out of the school's bus turnaround point,
18 which connects to the dirt access road that leads to the substation. This is a turn-around point
19 for school busses located behind the high school, removed from any streets, and does not
20 normally see traffic passing through, particularly in the early morning hours. At around
21 5:30 a.m., two individuals are observed walking on the dirt access road away from the
22 substation immediately following the loss of power. They are picked up by the same above-
23 referenced dark colored sedan, which then drives away from the scene. Due to the quality of
24 the surveillance video, the time of day, and the clothing the subjects wore, investigators have
25 been unable to identify suspects. The images below are snapshots of security camera footage
26 from the incident.
27
28



This substation is located down a dead-end road behind Woodland High School and is only reachable by a dirt access road. There is essentially no traffic, either vehicle or foot, that passes through the access road to the substation, especially during late night hours. A construction site is adjacent to the substation but is only active during business hours and was vacant at the time of the offense.

Location 2: 200 North Pekin Road Woodland, Washington

On November 18, 2022, unknown suspects caused damage to the electric substation located at 200 North Pekin Road, Woodland, Washington 98674. This substation is owned and operated by the Cowlitz Public Utility District and receives its electricity from the Bonneville Power Administration. It is responsible for distributing electricity to the town of Woodland and the surrounding areas.

On November 18, 2022, at approximately 4:30 a.m., unknown individuals forced their way under the barbed wire perimeter fence of the substation. Once inside the yard, the individuals broke a window to gain access to the control house.



Inside the control house, they manually manipulated the breakers that control the flow of electricity. The suspects also used a blunt object to smash the exposed, inner workings of the breaker towers, rendering multiple components inoperative and in need of either repair or replacement. This resulted in the interruption of electrical service for approximately 1,700 people and set-off alarms at the Cowlitz Public Utility District headquarters. The Cowlitz Public Utility District estimates that the damage caused by this incident was between \$50,000 and \$60,000.



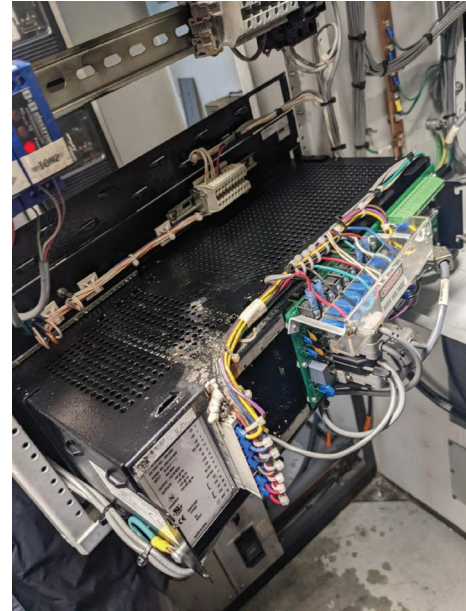
1 This substation is in a rural area, surrounded by woods and agricultural fields. As
2 such, there are no surveillance cameras in the area. A single, local road runs past the the
3 facility, which sees very little traffic during early morning hours.

4 **Location 3: 1007 39th Ave SE, Puyallup Washington**

5 On November 20, 2022, unknown suspects caused damage to the Fairchild
6 Substation, located in the vicinity of 1007 39th Avenue SW, Puyallup, Washington 98374.
7 This substation is owned and operated by Puget Sound Energy and receives its electricity
8 from the Bonneville Power Administration. It is responsible for distributing electricity to the
9 City of Puyallup.



20 During this incident, the unknown suspects breached the perimeter fence and forced
21 open the door to the control house. Once inside, they dumped transmission fluid on the
22 substation relays and other equipment and attempted to use flares to ignite the fluid. The
23 bottle of transmission fluid, a spray nozzle, and burned-out flares were found on scene.
24
25
26
27
28



FBI Special Agents interviewed PSE foreman Jared Corey. According to Corey, because the incident did not cause any power outages, it initially went undetected until a routine PSE inspection on November 22, 2022. Corey stated that the damaged electronics and control house equipment needed replacement and repair and estimated the cost would run into the tens of thousands of dollars. Corey assessed that this offense could have caused power outages for approximately 10,000 residential and commercial customers for an extended period, including to the Centeris data storage center, which provides services to several major companies, and the adjacent Kaiser Permeate medical facility.

After the damage was detected, PSE engineers determined that the attack most likely occurred on November 20, 2022, at approximately 4:05 a.m. At that time, the engineers detected a systems anomaly in transmissions from the substation to PSE's homebase. The performance abnormality was consistent with damage inflicted on the substation communication relay, where a flare was placed causing damage to the transmission box and melting surrounding wires.

The Fairchild substation is set back from the nearest roadway and bordered by trees on three sides. It is accessed only by a gravel road that leads off the nearest paved road. Beyond the trees, the substation area is bordered mainly by large parking lots and an

1 apartment complex. The area sees some traffic during the day, but very little at night while
2 local businesses are closed.

3 **Location 4: 1669 2nd Avenue SW, Tumwater, Washington**

4 On November 22, 2022, unknown suspects caused damage to the electric substation
5 located at 1669 2nd Avenue SW, Tumwater, Washington 98512. This substation is owned
6 and operated by Puget Sound Energy and receives its electricity from the Bonneville Power
7 Administration. It is responsible for distributing electricity to the city of Tumwater.



19 The unknown suspects damaged the Tumwater Substation using a firearm.
20 Specifically, the suspects shot three 9mm Luger rounds at the electrical equipment from
21 outside the perimeter fence. At 4:52 am., the local Puget Sound Energy Substation
22 Operations Inspector responded to an alarm that was triggered at the Tumwater Substation.
23 The inspector discovered fluid leaking from one of the radiator fins of the substation
24 transformer. The radiator had been punctured three times by what appeared to be bullet
25 holes.

26 A few minutes earlier, at 4:27 a.m., residents living near the Tumwater Substation
27 reported hearing three gunshots being fired in the area. Responding police officers
28

1 discovered three recently fired 9mm bullet casings along the perimeter fence of the
2 Tumwater Substation, approximately 35-40 feet away from the points of impact on the
3 transformer radiator.



4
5
6
7
8
9
10
11
12 Initial estimates from Puget Sound Energy are that the damage caused by this offense
13 is over \$250,000. The damage to the transformer caused a widespread power outage for
14 5,200 local residences for approximately 24 hours.

15 Investigators reviewed security camera footage from nearby businesses and
16 residences; however, those cameras did not capture individuals approaching or departing the
17 Tumwater Substation. As a result, investigators have not been able to identify the suspects.

18 The Tumwater Substation is located behind a Walgreens pharmacy, between a
19 roadway and Barnes Lake. Two sides of the substation are surrounded by empty fields,
20 bordered by thick trees. The roadway and surrounding area are active during the day, but see
21 little traffic at night while all local businesses are closed.

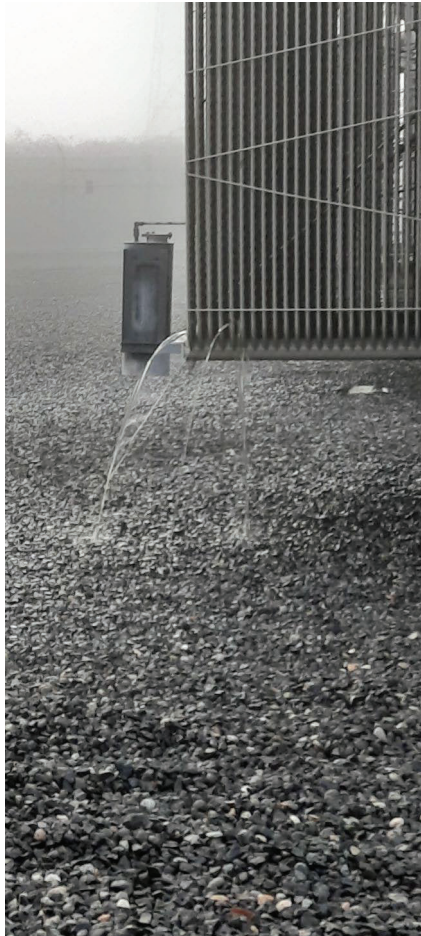
22 **Location 5: 16885 South Eaden Road Oregon City, Oregon**

23 On November 24, 2022, shortly after 1:00 a.m., unknown suspects caused damage to
24 the electric substation located at 16885 South Eaden Road Oregon City, Oregon. This
25 substation is owned by the Bonneville Power Administration. It serves as a critical main-grid
26 substation that directly connects and supplies power to four major BPA substations and one
27 major Portland General Electric substation. BPA's initial estimate is that the cost to repair
28 the damage is at least \$1,000,000.

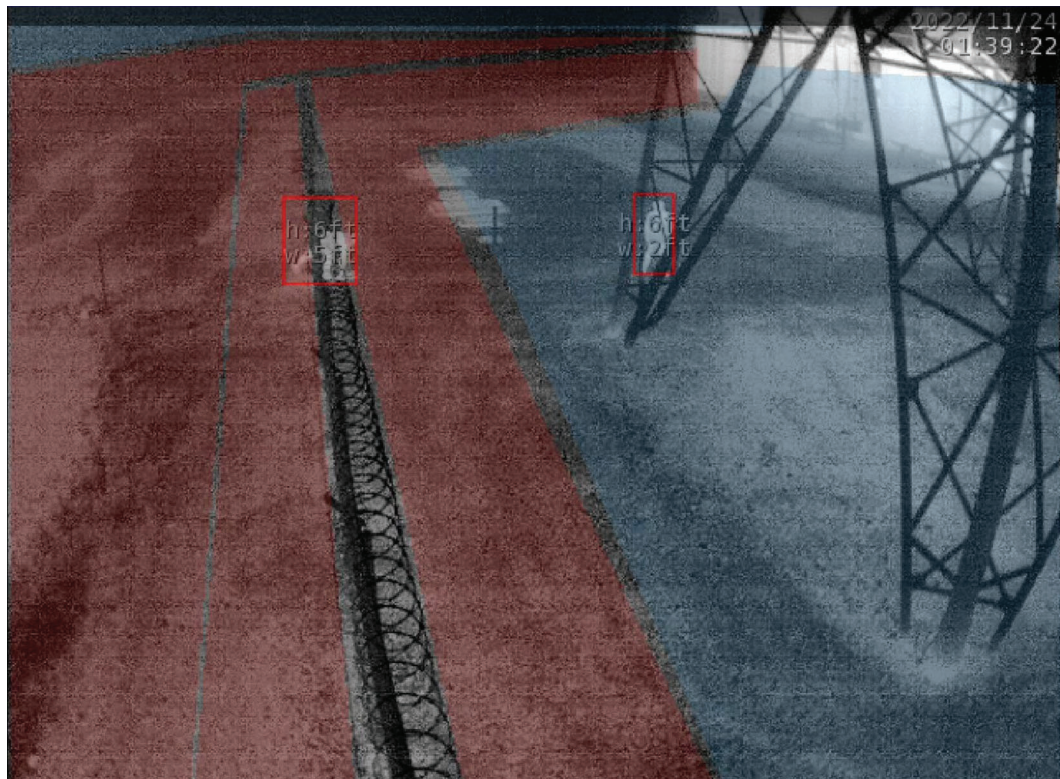
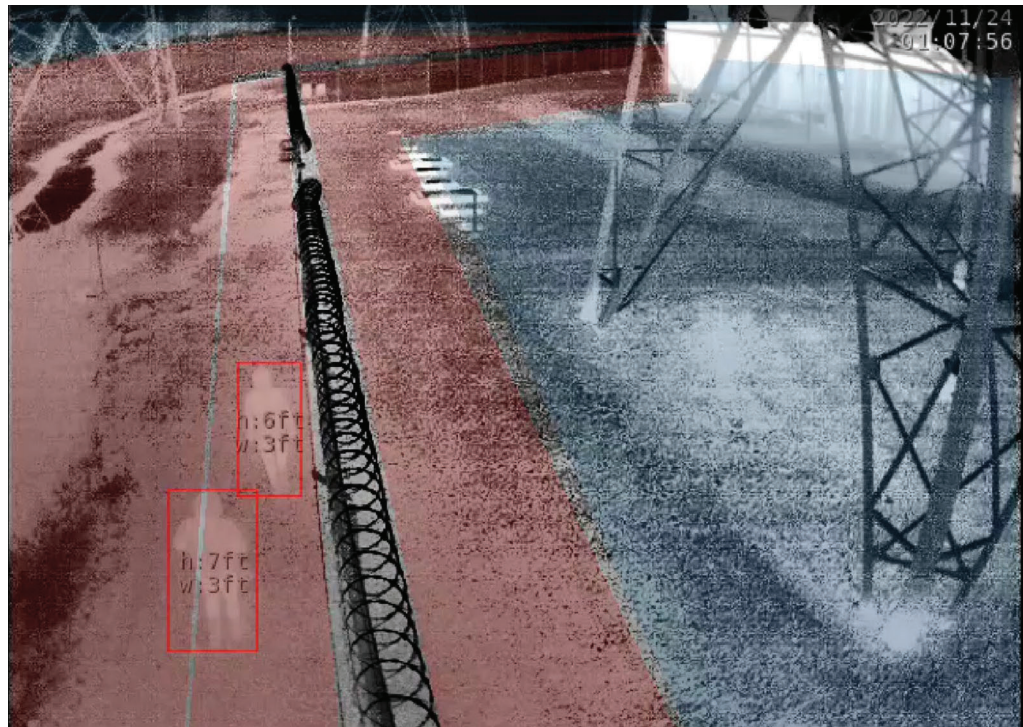
1 On November 24, 2022, at 1:06 a.m., BPA received an alert which indicated that a
2 motion alarm had been triggered at the Oregon City substation. The substation was equipped
3 with multiple infrared (IR) cameras that monitored the perimeter and fence. A BPA
4 employee checked the cameras and observed two heat signatures on the exterior of the
5 property. At approximately 4:00 a.m., BPA received a low-oil alarm from a separate system
6 that monitors the substation's electrical equipment. This system also indicated that some of
7 the substation's equipment was losing voltage on at least one reactor.

8 BPA dispatched substation operators to respond to the alarm. Upon arrival, they
9 discovered a hole cut in the perimeter fence of the energized yard and cooling oil leaking
10 from one of the reactor units. BPA employees alerted the Clackamas County Sheriff's
11 Office, and a Deputy was dispatched to the site. The Deputy discovered that the Phase A
12 reactor unit sustained three bullet holes to the cooling radiators, with oil leaking on the
13 ground. The Phase B reactor had one bullet hole and was also leaking oil. Investigators
14 recovered fourteen 9mm shell casings in the energized yard – twelve were found near the
15 reactor banks and two were found inside the yard near the hole in the fence.¹

16
17
18
19
20
21
22
23
24
25
26
27
28 ¹ The Clackamas County Sheriff's Office entered the 9mm casings into Integrated Ballistics Identification System (IBIS). There were no matches in the system. The 9mm casings were swabbed for DNA and the collection was sent to the Oregon State Police Crime Lab for analysis, which is still pending.



A review of the IR camera footage showed two suspects walking up and cutting into the perimeter fence at approximately 1:08 a.m. It took the suspects approximately 30 minutes to cut through the fence and gain entry to the yard.



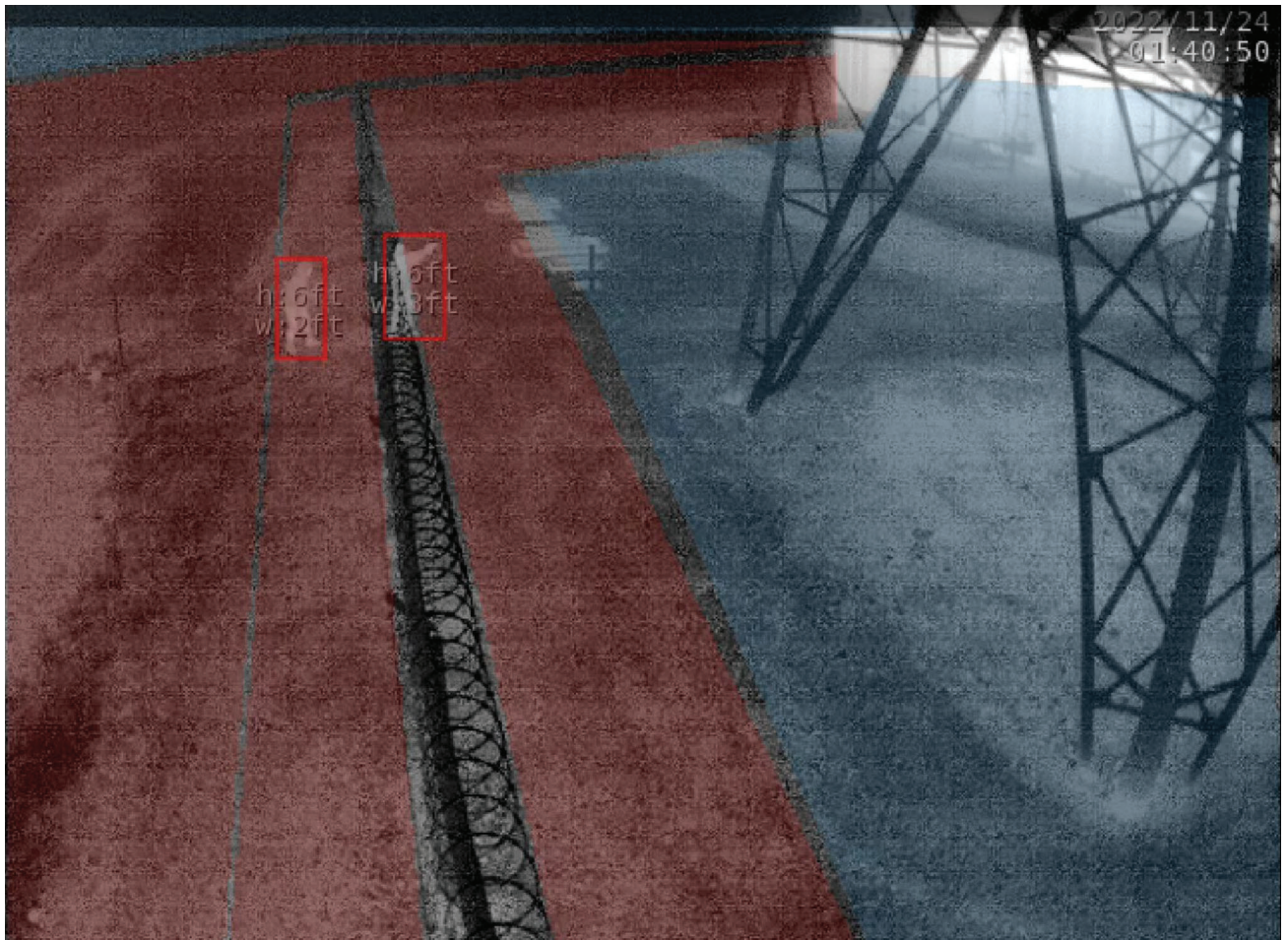
1 Soon after entering the yard, one of the two suspects holds an object in the air and
2 walks around the yard with it for approximately one minute. Investigators believe this object
3 to be a cellular phone that the subject is using to take a video or photographs. The belief that
4 the object is a phone – instead of another item – is based on the facts that: the manner in
5 which the suspect holds the item with one hand, keeping it still for several moments, is
6 consistent with taking a video or photograph; the area where the suspect was standing was
7 well-lit by flood lights, so there was no need for the suspect to use a flashlight or similar
8 device; there were no shell casings recovered in this area; and the manner in which the
9 suspect holds the device is not consistent with a firearm.

10 The suspects continued to move west across the yard and exited the field of view of
11 the camera approximately fifteen feet from where twelve of the 9mm shell casings were
12 recovered. About one minute later, the suspects reenter the camera's view and are seen
13 running across the yard back to the hole in the perimeter fence.

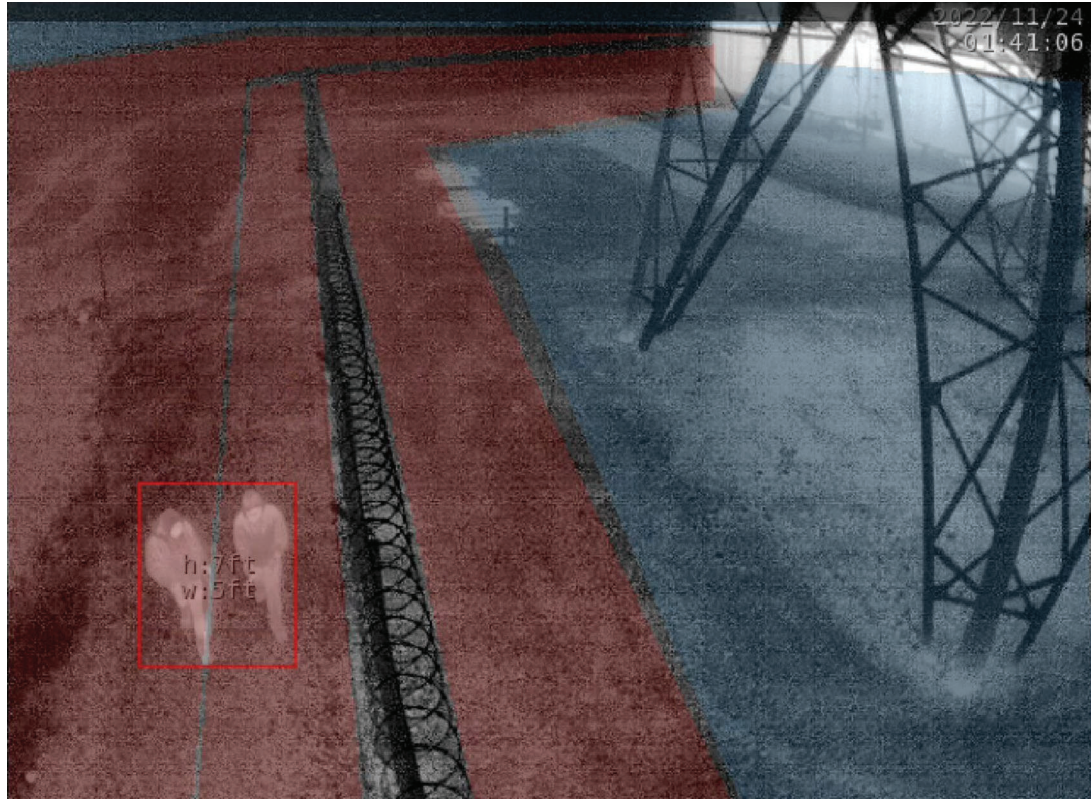


27 The camera footage shows one of the two suspects stopping before climbing back
28 through the fence. The suspect raises an object in the air; the outline of this object resembles

1 a firearm. This is the same location where two of the 9mm shell casings were recovered. As
2 a result, investigators believe that the suspect fired at least two rounds at this time.



19
20 At approximately 1:41 a.m., the subjects are seen walking north along the exterior of
21 the perimeter fence in the direction of the main access road for the substation.
22
23
24
25
26
27
28



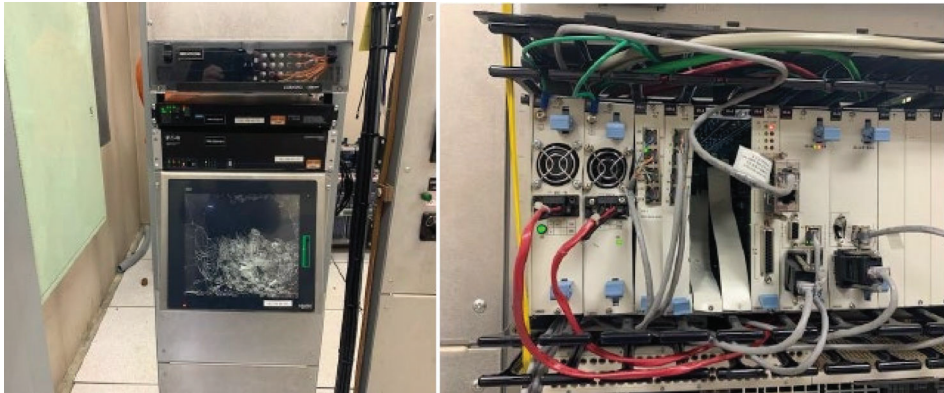
The Oregon City substation is in a remote, rural area. The substation is surrounded by agriculture fields and wooded areas. There is virtually no traffic that passes close to the substation, either vehicle or foot, at any time of day or night.

Location 6: 8396 SE Sunnyside Road Clackamas, Oregon

On November 28, 2022, at approximately 12:49 a.m., unknown suspects caused damage to the electrical substation located at 8396 Southeast Sunnyside Road Clackamas, Oregon. This substation is owned and operated by Portland General Electric. The damage caused by the suspects de-energized the substation's two transmission sources, resulting in a power outage to 6,337 industrial, commercial, and residential customers in the Clackamas area.

During this incident, two unknown suspects cut through a perimeter fence and gained entry to the yard. Once inside the yard, the suspects broke into the control house. Using a blunt object, they smashed the exposed, inner workings of the supervisory control and data acquisition system ("SCADA"), which controls industrial processes such as the gathering of

1 data in real time from remote locations to control equipment and conditions. The attackers
2 also damaged a computer screen and other equipment rendering multiple components
3 inoperative and in need of repair or replacement. According to Portland General Electric, the
4 offense caused a power outage in the surrounding area and damages of approximately
5 \$26,000.



24 The Clackamas County Sheriff's Office responded to the scene and obtained
25 security camera footage from a nearby business. FBI agents reviewed the video and observed
26 that at approximately 12:37 a.m., at least two unknown suspects entered the camera view
27 wearing dark clothing. They approached the substation's exterior fence near where it had
28 been cut open. One of the suspects crouches down by the fence for several minutes. At

1 approximately 1:02 a.m., one of the suspects appears to climb through the fence and walks
2 towards the substation control room building, which was ultimately damaged. The video
3 ends at 1:05 a.m.

4 This substation is in a populated area with arterial roadways on the north and west
5 sides. The substation is surrounded by businesses. However, none of the business were open
6 from midnight to 2:00 a.m. at the time of the attack. The roadways and surrounding area are
7 active during the day but see little traffic at night while all local businesses are closed.

8 **Connections Between the Attacks at the Substations**

9 Based on the FBI's investigation to date, I submit there is probable cause to believe
10 that the six incidents under investigation are part of a conspiracy to damage electrical
11 substations in Southwest Washington and Northwest Oregon. There are several reasons to
12 believe that these incidents are related as part of a conspiracy.

13 First, the tactics used by the suspects are consistent with the methodologies called for
14 by the Hard Reset publication. Specifically, the various attacks have used means of firearms,
15 arson, damaging substation control house equipment, and causing leaks to oil tanks, all of
16 which are specifically outlined in the Hard Rest.

17 Second, for each of the incidents where surveillance camera footage is available
18 (Locations 1, 5, and 6), there appeared to be two suspects who were wearing dark clothing.
19 These incidents spanned both the Western District of Washington and the District of Oregon.

20 Third, the means used by the suspects were consistent across certain incidents. For
21 example, the attacks at Location 4 (Tumwater, Washington) and Location 5 (Oregon City,
22 Oregon) involved the use of firearms to shoot holes in the substation radiators, causing oil to
23 leak. Moreover, both attacks were committed using a 9mm firearm. Likewise, the attacks at
24 Locations 1 and 2 (Woodland, Washington) and Location 6 (Clackamas, Oregon) were
25 similar in that the suspects broke through the substation perimeter fences, broke into the
26 control houses, and used blunt objects to damage the electrical equipment, causing power
27 outages.
28

1 Lastly, BPA employees have told the FBI that the number of attacks in this type of
 2 concentrated period is highly unusual. This suggests that the attacks are part of a coordinated
 3 effort as opposed to random individual events.

4 **Returns on the Original Cell Tower Warrant**

5 This warrant request is a follow-up to the prior cell tower warrant issued by this
 6 Court. On December 16, 2022, Magistrate Judge J. Richard Creatura issued a geofence and
 7 tower dump warrant in case MJ22-5295. On January 30th, 2022, the FBI received the returns
 8 from T-Mobile, in case reference number 4163401.

9 The returns provided telephone numbers and unique identifiers for each wireless
 10 device in the vicinity of the identified cell towers, the sectors that received a radio signal for
 11 each communication, and the date, time, and duration of each communication. The returns
 12 only identified cellular devices that had connected to the cellular towers and utilized them for
 13 active SMS and phone calls. The returns identified the location of these devices by sector,
 14 but not by distance from the towers.

15 The returns did not include devices that connected to the towers using timing advance
 16 data. Were that data included, the number of responsive devices would be larger, as not
 17 every cellular device that connects to a tower sends active SMS or call data while connected.
 18 By requesting timing advanced data in this warrant, we expect the returns to provide
 19 significantly more investigative leads than the original cell tower data returns.

20 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

21 Based on the foregoing, I request that the Court issue the proposed cell tower search
 22 warrants pursuant to 18 U.S.C. § 2703(c). I further request that the Court direct T-Mobile, to
 23 disclose to the government any information described in Section I of Attachment B that is
 24 within their possession, custody, or control.

25 As described in Attachment A, the requested warrant would require the disclosure of
 26 records and information relating to the cell towers providing service at the following
 27 locations, including all the cellular telephone numbers whose timing advance data places
 28 them with a one-half mile radius from the below locations.

| Location | Date | Times |
|---|----------------------|---|
| The cell towers that provided cellular service to 2210 Robinson Road, Woodland, WA 98674 | November 17, 2022 | 3:30 a.m. – 3:45 a.m. (PST) 5:00 a.m. – 6:00 a.m. (PST) |
| The cell towers that provided cellular service to 220 North Pekin Road, Woodland, WA 98674 | November 18, 2022 | 4:00 a.m. – 5:00 a.m. (PST) |
| The cell towers that provided cellular service to 1007 39 th Avenue SE, Puyallup, WA 98374 | November 19-20, 2022 | 11:00 p.m. on November 19, 2022, through 5:00 a.m. on November 20, 2022. |
| The cell towers that provided cellular service to 1669 2 nd Avenue SW, Tumwater, WA 98512 | November 22, 2022 | 3:45 a.m. – 5:00 a.m. (PST) |
| The cell towers that provided cellular service to 16885 South Eaden Road, Oregon City, OR 97045 | November 24, 2022 | 12:50 a.m. to 1:50 a.m. (PST) |
| The cell towers that provided cellular service to 8396 SE Sunnyside Road Clackamas, OR 97015 | November 28, 2022 | 12:30 a.m. to 1:10 a.m. (PST) |

REQUEST FOR SEALING

I further request this Court issue an order sealing all papers submitted in support of the requested search warrants, including the application, this affidavit, the attachments, and the requested search warrants. I believe sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause the culpable person(s), or others associated with the culpable person(s) to flee from prosecution, cause destruction of or tampering with evidence, or otherwise seriously jeopardize this investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrants may adversely affect the integrity of the investigation.


CONCLUSION

Based on the forgoing, I request that the Court issue the proposed warrants, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703.

Pursuant to 18 U.S.C. § 2703(g), the government will execute the warrants by serving the warrants on T-Mobile. Because the warrants will be served on these providers, who will then compile the requested records and data, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night. I therefore further request that the Court authorize execution of the warrants at any time of day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants.

Accordingly, by this affidavit and application I seek authority for the government to seize the items specified in Attachment A (attached hereto and incorporated by reference herein) to the warrants. I further request that the Court direct T-Mobile to disclose to the government any information described in Attachment A that is within their possession, custody, or control. I also request that the Court direct these providers to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment A unobtrusively and with a minimum of interference with its services.

1 I declare under penalty of perjury that the statements above are true and correct to the
2 best of my knowledge and belief.
3
4

5
6 
7 SAMUEL WHARTON
8 Special Agent, FBI

9 The above-named agent provided a sworn statement to the truth of the foregoing
10 affidavit by telephone on the 17th day of March, 2023.
11

12 
13 THERESA L. FRICKE
14 United States Magistrate Judge
15
16
17
18
19
20
21
22
23
24
25
26
27
28